BY ORDER OF THE COMMANDER
AIR FORCE MATERIEL COMMAND

AIR FORCE INSTRUCTION 33-202

AIR FORCE MATERIEL COMMAND
Supplement 1

30 AUGUST 2002

Communications and Information

COMPUTER SECURITY

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the HQ AFMC WWW site at: https://www.afmc-mil.wpafb.af.mil/pdl/

OPR: AFMC CSO/SCON (Mr. Coston Smith) Certified by: AFMC/SC (Colonel Rebecca Corder)
Supersedes AFI 33-202/AFMCS1, 23 May 00 Pages: 20
Distribution: F

This supplement defines criteria for computer security (COMPUSEC). Base supplements can add to but not take away from the Air Force Instruction (AFI) and major command supplement. This supplement applies to all AFMC organizations. It also applies to all other organizations and contractors residing on an AFMC base or geographically separated unit (GSU) using computer equipment. It also applies to all organizations connected directly, physically or logically, to the base network.

AFI 33-202, 30 August 2001, is supplemented as follows:

2.5.3. The term Single Manager is clarified to include program manager or project manager.

2.5.3.2. The Single Manager will as a minimum coordinate with the Designated Approving Authority (DAA) to obtain interim accreditation prior to Initial Operating Capability. An accredited System Security Authorization Agreement (SSAA) (interim or final) will be provided to applicable Base Information Assurance (IA) office prior to operation of system.

2.5.3.2.1. (Added) Prior to installing new systems on the network, coordinate with the Base Information Assurance Office to schedule an Internet Security Scanner (ISS) scan.

2.5.3.13. Also coordinate the development of information systems with the applicable Unit Computer Security (COMPUSEC) Manager (UCM) early in the acquisition and development process.

2.5.3.14.1. (Added) May perform certifier (AFI 33-202, paragraph 2.8) functions under Memorandam of Agreement (MOA) with the requiring functional.

2.10.1.2. The Wing/Base IA office will notify the MAJCOM IA office, in writing, of the name, grade, DSN, commercial telephone, FAX number, e-mail, and mailing address of primary point of contact (POC) for compliance with Certification and Accreditation (C&A) requirements. This information shall be updated as soon as any changes occur.

2.10.1.2.1. (Added) Track and maintain all accreditation information and notify DAAs of reaccreditation due dates no later than six months prior to the reaccreditation date.

2.10.1.4. Whenever practical, the Base Information Assurance Office (BIAO) will run an ISS scan on new automated information systems (hardware and software) prior to systems being installed on the operational network. In cases where the ISS scan can not be accomplished prior to installation, the BIAO will conduct the ISS scan of new systems not later than 24 hours after the new system has been installed on the network.

2.10.1.5. Internet Protocol (IP) addresses shall not be issued until the Wing/Base IA office determines that the system has been subjected to penetration testing and is accredited.

2.10.1.7. (Added) The Wing/Base IA office will provide training to newly assigned UCMs and hold annual meetings with the managers. The training and meetings shall be documented. At a minimum, the Wing/Base IA office will maintain records of personnel trained, date of training, office symbol, and telephone number.

2.10.1.8. (Added) The Wing/Base IA office will ensure that a National Security Agency (NSA) approved degausser is located on the base and is available for use**.**

2.10.1.9. (Added) Wing/Base IA office will review/update the DAA information at least semi-annually to ensure currency. Identify each organization within the accreditation boundary as tenant, Wing, or GSU in order to determine DAA assignments as established in section 3.2.

2.11.1.7. (Added) HQ AFMC directorates will appoint UCMs to support their respective DAA functions. Notification of appointments will be made in writing to their respective Wing/Base IA offices. The UCM and Information System Security Officer (ISSO) will not be in the MAJCOM or Wing/Base IA office to avoid a conflict of interest.

3.2.1. The highest Base authority (Air Base Wing or Center commander) is the site accreditation DAA. All systems attached within the site accreditation boundary must have a security risk assessment review by the Wing/Base IA office, to include packages prepared by tenant units. For clarification purposes, stand-alone systems (referred to in paragraph 3.2.1 in the basic AFI), apply to host base versus tenant systems.

3.2.1.2.1. (Added) The highest Base authority (Air Base Wing or Center commander) may appoint DAA representatives. The DAA representative must ensure that the Wing/Base IA office reviews all certification and accreditation risk analysis packages. Recommendations for approval/disapproval will be provided to the DAA representative. If recommended for disapproval by the Wing/Base IA, the areas of concern must be fixed and package approved prior to connection and/or operation on the base network. The requester and Wing/Base IA offices will maintain copies and records of package approval/disapproval and re-certification requirement dates.

3.2.1.2.2. (Added) DAA or DAA Representatives must be appointed via memorandum to the Wing/Base IA office to include the appointees name, grade, organization/office symbol, DSN, commercial telephone, FAX numbers, e-mail, and mailing address. This information must be updated immediately upon any change of the submitted information.

3.2.2. For clarification purposes, tenant unit commanders are DAAs for unique systems and networks that are not connected to the base network (i.e., stand-alone systems).

3.2.2.1. (Added) HQ AFMC 2-Letter Functionals. The HQ AFMC 2-letter/deputy levels have DAA authority to type accredit classified and unclassified systems under their jurisdiction.

3.5.1.1.1. (Added) In order to facilitate granting contractor access to AFMC networks, it is important that requiring organizations and contracting offices understand the identification and screening requirements for contractor personnel. The acquisition authority must ensure that these requirements are addressed during acquisition planning and incorporated into pre-award contract documentation. The requirements must also be included in any Request For Proposal (RFP) or Invitation for Bids (IFB) to inform potential offerors/bidders of the investigative and Designated Approval Authority (DAA) access approval requirements. These requirements must continue to be enforced throughout the duration of the contract.

3.5.1.1.1.1. (Added) DAAs must ensure supervisors, unit COMPUSEC personnel, and Work Group Managers/ Functional Systems Administrators understand that contractors require personnel security investigations National Agency Checks (NAC) or Single Scope Background Investigations (SSBI) for access to government e-mail/network/computer systems and that DAA approval is required prior to establishing a contractor user account. The unit computer security manager will not sign an access form for a contractor's final access until the unit security manager confirms that a personnel security investigation has been completed and DAA approval granted. In addition, unit computer security managers will not sign an access form for interim access by a contractor until (1) Security Forces personnel have completed a Local Files Check (LFC) with no adverse results, (2) the ISPM has submitted a request for a personnel security investigation of the appropriate level (NAC or SSBI), and (3) the DAA has approved interim access. Temporary hire (less than 180 day) personnel must have a completed LFC with no adverse information and DAA approval for interim access. User access to information system resources must conform to personnel security requirements identified in AFSSI 5027 and AFI 31-501.

3.5.1.2.1. (Added) Systems must conform to accreditation requirements IAW AFI 33-202, Chapter 4.

3.5.1.3.1. (Added) Users will activate password-protected screensavers when workstations are left unattended for any period of time and not powered down.

3.5.1.3.2. (Added) Users must ensure screensaver passwords conform to password standards outlined in AFSSI 5027.

3.5.3. Guidance on the use of Personal Digital Assistance (PDA): See Attachment 1 for updated policy.

3.5.3.9.5. (Added) Anti-virus/scanning software will be installed on PDAs prior to being issued to users. Updates will be conducted as a minimum IAW AFI 33-202, paragraph 3.13 and this supplement.

3.7.1. All Foreign National requests not specifically covered by paragraph 3.7.3 of the basic AFI (such as access by foreign nationals from within their country) will require AFMC/CV approval. Access request packages will be submitted to HQ AFMC IAW Attachment 4, Guide/Format.

3.7.1.1. (Added) Access will be limited to the extent necessary to perform assigned duties. [**Note:** approval to access the Unclassified but Sensitive Internet Protocol Router Network (NIPRNET) or other networks by foreign personnel does not equate to authority to exchange data or access systems located on that network].

3.7.3. All foreign national email accounts must include the individual's last name, first name, rank, country of origin, organization (e.g. Boyd, Anthony, WG Cdr, UK, AF/SCX). Information Assurance awareness training remains in effect for all personnel. Prior to arrival of personnel to assignment, the following actions should be taken:

- Supervisors of personnel will identify specific Automated Information System (AIS) access requirements for the position.

- •The local foreign disclosure officer will validate that the Foreign National access requirements fall within the limits of the disclosure authority approved for the position.
- •Supervisors of personnel will work with the Unit COMPUSEC Manager and/or ISSO to implement necessary controls to assure that only authorized AISs are accessible by foreign personnel, as defined by the foreign disclosure officer.
- •Supervisors of foreign personnel will ensure personnel access to any unclassified information system/website containing information that is controlled under the arms export control act, privacy act, and exemptions to the freedom of information act, is approved by the system DAA and is reviewed by the local foreign disclosure officer.

3.7.3.1. A number of United States (US) computer systems containing ***"country data"*** exist within HQ/AFMC. When foreign nationals/representatives outside CONUS require access to their country's data resident in a US computer system, they must complete and sign a system authorization access request (SAAR) form. In order to gain access to a US computer system, foreign nationals/representatives must validate the sponsorship of their government by completing a security form for Foreign Military Sales (FMS). The FMS security assurance must be signed/authenticated by and forwarded to the security manager of the applicable AF data system from the embassy in Washington D.C., in order for that user requesting access to receive information on behalf of that government. Authentication must include the level of data required and the level of clearance granted by that country to that individual. This security assurance will be maintained by the security manager of the applicable AF data system along with the users SAAR form.

3.7.3.2. The system(s) accommodating the foreign national(s) must be certified and accredited. The risk analysis must recognize that foreign nationals are accessing the system's information and identify the measures in place to ensure only authorized information is accessed.

3.7.3.3. Access to systems must take into account disclosure limitations that limit liaison personnel to information pertinent to their country's purchase of goods or services under contract to the U.S.

3.7.3.4. As noted above in paragraph 3.7.3, the foreign national's e-mail address must identify them as a foreign national. Further, browser capabilities which allow access to the internet via e-mail services must be restricted/disabled.

3.7.3.5. Stand-alone systems/local area networks (LANs) (no base backbone connectivity) used specifically for foreign nationals located on AF installations or sponsored by their government may provide Internet connectivity via commercial ISP. Connections(s) may be dedicated or dial-up and in this instance the foreign nationals shall not advertise or use ".mil" addresses.

3.13.1.5. (Added) The base network control center (NCC) will automate anti-virus update procedures on all networked computers. The automated tool/script will be configured to ensure the update is loaded prior to completion of user login. It will be set up to minimize interaction by the user. At the most, the user should only need to press enter to reboot.

3.13.2.1. (Added) Block infected emails and/or attachments at the firewall/base router.

3.13.2.2. (Added) Disconnect external access to base e-mail server(s) until all infected e-mails are deleted from the server(s) and the appropriate anti-virus update software is loaded onto the server(s) and applicable workstations.

3.13.3.1. For clarification virus scans will be conducted daily IAW the basic AFI and the Internet Security Scanner (ISS) will be conducted on a quarterly basis at level 3 and level 5 annually.

3.17. Guidance on Wireless Local Area Networks (WLAN)

3.17.1. All client devices using the base wireless infrastructure will meet the following security requirements:

3.17.1.1. (Added) Wireless client devices must be registered with the NCC prior to connecting to the base wireless infrastructure. At the time of registration, the NCC will record a device-specific authentication factor – usually the Media Access Control (MAC) address of the device – to be used for hardware authentication. This address will be added to the access control lists of appropriate access points.

3.17.1.2. (Added) Lost or stolen wireless devices must be reported to the NCC immediately within 24 hours. Entries for such devices will be removed from all access control lists. If recovered, the device-specific authentication factor will be considered compromised and must be changed before the device is redeployed.

3.17.1.3. (Added) All wireless client devices must run AF-approved anti-virus software.

3.17.1.4. (Added) All wireless client devices must use the VPN system client (usually software)

compatible with the VPN system managed by the NCC.

3.17.1.5. (Added) Wireless client devices will not allow ad hoc wireless networking or direct peer-to-peer wireless networking [e.g., Bluetooth and infrared (IR)].

3.17.1.6. (Added) Systems with direct network access (e.g. via Ethernet cable) shall not provide wireless data connectivity of any sort. This includes wireless control pads and wireless keyboards.

3.17.1.7. (Added) WLAN Encryption.

3.17.1.7.1. (Added) All traffic transmitted via WLAN must be encrypted using FIPS 140-1/2 Triple-DES, 128-bit key length or better.

3.17.1.7.2. (Added) Wired Equivalent Privacy (WEP), Dynamic WEP or WEP+ will not be used to provide the primary session encryption. WEP may be used in addition to the encryption required in item (1) above.

3.17.1.7.3. (Added) The VPN system will originate at the client device and will terminate outside the base network boundary so that traffic from the wireless network will traverse the NCC-controlled firewall “in the clear”.

3.17.1.8. (Added) WLAN Access Points

3.17.1.8.1. (Added) No access point will connect directly to the trusted internal network infrastructure. Such access points will be treated as back doors to the network and must be removed immediately.

3.17.1.8.2. (Added) All access points will connect to a VPN system located outside the trusted internal network. This connection may be physical, or an NCC-established VLAN.

3.17.1.8.3. (Added) Access points will be configured to limit broadcast to only registered wireless devices.

3.17.1.9. (Added) DHCP servers will issue IP addresses only to registered wireless client devices.

3.17.1.10. (Added) User authentication will be performed by the established network domain server(s).

3.17.1.11. (Added) The following firewall policy applies to WLAN systems.

3.17.1.11.1. (Added) All wireless access points will connect physically or logically to a VPN device located outside of the trusted internal network. The VPN device will connect to an NCC-controlled firewall.

3.17.1.11.2. (Added) The VPN will not connect to the DMZ. Wireless traffic must remain isolated from Internet and NIPRNET traffic.

3.17.1.11.3. (Added) VPN device will connect to an isolated interface of the established firewall. This interface may be the existing RAS interface.

3.17.1.12. (Added) SSAA's will depict the WLAN architecture.

3.17.1.13. (Added) Refer to Attachment 1 for additional AF/SC policy.

3.18. (Added) Policy Compliance Violations.

3.18.1. (Added) Command Network Control Center (CNCC)/Wing/Base IA personnel will review ISS, War Dialer results, audit records, etc. to enforce policy compliance in areas noted in IA Violation Decision Matrix (Attachment 2).

3.18.1.1. (Added) Organizational Commanders will use Attachment 2 to develop a local set of corrective IA actions to ensure network security is maintained. Outside of this matrix, commanders should consider taking administrative or disciplinary actions in appropriate cases. **Note:** Civilian personnel actions must comply with Attachment 3 of AFI 36-704, *Guide to Disciplinary Actions*.

3.18.1.2. (Added) Analysis will be performed on the data and actions taken to ensure unauthorized high bandwidth (those sites that could create a denial of service situation) sites are blocked at the firewall and/or router.

3.18.1.3. (Added) Any extended/repeat visits to or downloading of material from unauthorized sites by individuals will be reported via memorandum to the organization of the offending individual(s) for proper action. The report will be via a formal memorandum (example at Attachment 3) to the offender's organization. Ensure copy is provided to Communication Unit and Security Forces Commander for their appropriate action.

3.18.2. (Added) The CNCC will logically and/or physically disconnect from the base network any subnet or computer that does not have a full or interim C&A approved by the base network DAA.

3.18.2.1. (Added) If the organization has not completed recertification by the expiration date, the CNCC will disconnect the subnet(s)/computer(s) from the base network IAW AFI 33-115 V1, paragraph 6.4.3.4.1.1.

3.18.2.2. (Added) Any external unauthorized connection to LAN or computers connected to the base network will either be disconnected or result in the disconnection of the offending subnet(s) and/or computer(s) IAW AFI 33-115, paragraph 6.4.2.4 and paragraph 6.4.3.4.1.1.

3.18.2.3. (Added) Any activity that is non-compliant with Air Force, AFMC or local network operations and security policy will be disconnected. The only exception to this guidance would be if technical problems prevented its implementation. In this case, the non-compliant user/organization will submit a waiver request via the base DAA to MAJCOM SC for appropriate staffing/approval. Waiver requests will document the technical reasons for non-compliance and describe all efforts being taken to mitigate network risk/vulnerabilities.

3.19. (Added) Account, Login, and Password Management

3.19.1. (Added) Strong password use shall be the standard authentication method employed throughout the Command. To enforce strong authentication, passwords must be at least eight characters long and include at least one character from each of the four character sets (upper case letters, lower case letters, numbers, and special characters such as ? / %). Additional guidance may be found in AFM 33-223, Identification and Authentication, and corresponding AFMC Supplement 1. Enforcement of these requirements is operating system dependent; therefore, for operating systems with inherent password enforcement capabilities (i.e., such as Microsoft Windows NT and 2000), appropriate resource kits and/or policy settings shall be used. Otherwise, for those operating systems without such capability (i.e., Unix), a commercially available automated tool for developing and enforcing strong password generation shall be purchased, installed, and implemented.

3.19.2. (Added) Users will activate password protected screen savers any time they leave their workstation unattended. All systems will be configured to provide the ability to activate password-protected screensavers.

3.19.3. (Added) During elevated Information Conditions (INFOCONs), abide by appropriate INFOCON requirements for duration of passwords and other password change requirements.

3.19.4. (Added) System administrators shall employ one of two account types: system administrator account and standard user account. Default system administrator accounts must be disabled after building a mandatory alternative account with system administration privileges. System administrators shall use this alternative account only to engage in network administration activities. The identifier for this alternative system administers account shall be built using a combination of the administrator's first, last, and/or middle name and will not contain any reference to the system administrator title. For non-administrative network access, the system administrator shall use a standard network user account that is significantly different from his/her system administrator account. Both accounts shall comply with the requirements for strong passwords (see paragraph 3.19.1). Additional guidance may be found in AFI 33-115, V1, Network Management.

3.19.4.1. (Added) Passwords will be changed at intervals not to exceed 90 days.

3.19.4.2. (Added) User's Remote Access Server (RAS) dial-up password must be different than any other password to base resources/network.

3.19.4.3. (Added) Passwords for RAS, system administration, and user accounts must all be different. No two passwords for an individual user may be the same.

3.19.5. (Added) Users will log off/turn off their computers at the end of each workday, unless the NCC requests otherwise.

3.19.6. (Added) Ensure controls are in place to monitor the use and provide timely disable/removal (within 3 days) of user accounts from the system or network, upon account termination or when necessary (i.e., disgruntled employee, change in contractors, 57-day inactive account, etc.).

Attachment 1 (Added)

22 October 200

MEMORANDUM FOR ALMAJCOM-FOA-DRU/SC

FROM: AF/SC

SUBJECT: Air Force Policy for Wireless Local Area Network (WLAN) and Personal Digital Assistant (PDA) (AF/SC Policy Memorandum 10-1-2001)

Commanders and functional communities have quickly embraced WLANs and PDAs as viable means to improve mission accomplishment, extend network range, and increase personal productivity. We've just updated our policy (atch 1) -- effective immediately -- to further define and clarify how WLANs and PDAs fit into the *One Air Force...One Network* enterprise. We need your help to ensure enterprise-wide understanding and compliance with this new policy (special target: Designated Approval Authorities).

We've included a briefing (atch 2) C&I commanders can use locally to educate base level people. Please send lessons learned and suggested improvements to AFCA/GC. Additional information is available at https://www.afca.scott.af.mil/category4.html or through Major David Frye (AF/SCMN, DSN 425-6148) or Mr. Carlson Wiltshire (AF/SCMN, DSN 425-2559).

//signed//

JOHN L. WOODWARD, JR., Lt Gen, USAF
DCS/Communications and Information

Attachments:
1. AF Policy for WLAN and PDA
2. Policy Briefing

Air Force Policy for Wireless Local Area Network (WLAN)

And Personal Digital Assistant (PDA) 10 October 01

This policy provides guidance to implement WLAN/PDA capabilities and mitigates risks from known operational and security problem areas. This policy remains in effect until revoked or superseded.

Section 1 - WLAN

1. Application:

Applies to wireless capabilities and devices connecting to AF Networks.

2. Operations:

a. WLAN must meet the same requirements of security, manageability, and scalability as wired networks.

b. Comply with AFMAN 33-120, *Radio Frequency (RF) Spectrum Management, par* 4.21. Nonlicensed Devices. A nonlicensed device is a low power intentional, unintentional or incidental radiator or device that meets the technical specifications prescribed in FCC Code of Federal Regulation, Title 47, Part 15 or the NTIA Manual Annex K. Nonlicensed devices are afforded no protection from interference. If interference is caused to an authorized service, the non-licensed device must cease operation. Because of this, AF activities must exercise caution in procuring and using non-licensed devices. Examples of non-licensed devices are wireless local area networks, wireless microphones, and cordless telephones. Using activities will not indiscriminately use non-licensed devices for critical command and control applications essential for mission success, protection of human life or high value assets.

c. Comply with AFI 33-118, *Radio Frequency Spectrum Management, par* 4.2.1. Non-licensed devices must conform to the FCC Rules, Part 15 or technical criteria in NTIA Manual. These devices include (but are not limited to) wireless local area networks, wireless barcode readers, bio-medical telemetry, and cordless telephones. AF activities will not indiscriminately use non-licensed equipment for critical tactical or strategic command and control applications essential for mission success, protection of human life, or protection of high-value assets, as they offer no protection of spectrum use in support of operational requirements.

d. Existing WLANs may continue to operate, but the responsible designated approving authority (DAA) must develop a local WLAN migration plan to meet wireless security requirements in AFI 33-202, *Computer Security*, NLT 1 Jan 03.

3. Security:

Use caution in implementing 802.11 security elements, and do not rely solely on inherent security mechanisms of the standard due to known vulnerabilities and exploits. If the inherent security is the only technically feasible solution, then additional compensatory measures must be implemented. From a security point of view, it's preferable to have separate keys for encryption and authentication. Another mechanism to ensure privacy through encryption is to use a virtual private network (VPN), which provides end-to-end encryption through tunnel mode IPSEC.

Bottomline, provide the strongest level of security available and ensure effective security management from a central point of control.

Information transmitted over a WLAN must be encrypted. Keep in mind the majority of COTS RF WLAN products do not provide policy-compliant encryption (even for sensitive, but unclassified data).

a. Base WLAN authentication must be based on device-independent items (such as user names and passwords), which users possess and use regardless of the clients they use.

b. Must support mutual authentication between a client and authentication server.

c. Use wired equivalent privacy (WEP) keys that are generated dynamically upon user authentication. At a minimum, users are advised that WEP must be enabled to use strong password protection and strong data encryption. Recent studies have shown WEP to be basically insecure with its current implementation of static keys, because the majority of access points are being deployed without WEP enabled).

d. Implement passwords according to AFMAN 33-223, *Identification and Authentication.*

e. Configure systems as a subnet to an existing network.

f. IR WLANs are permissible when implemented in accordance with AFI 33-203, *Emission Security.*

g. WLAN operation must adhere to the requirements and responsibilities IAW AFI 33-201, *Communications Security* (COMSEC), and the component of information assurance.

h. Future capabilities must comply with AFI 33-202, *Computer Security* mandating WLAN security policy.

(1) For encryption of classified information use National Security Administration (NSA) endorsed Type 1 products.

(2) For encryption of unclassified but sensitive information (SBU), utilize NSA endorsed products or a hardware or software VPN to secure the wireless to wired infrastructure that is based on IPSEC protocol with FIPS 140-1 / 140-2 validation for the underlying crypto module.

As part of fielding a new WLAN system, the new system must provide the baseline SSAA to include the wireless access points to the wired network and the wireless devices per the accreditation boundary for the system. The following are steps to follow when collocating access points: As with installing any access points, ensure that you accomplish a RF site survey to ensure the location of the access point will provide adequate coverage. Set each access point to a different frequency channel. The 802.11b standard defines 14 channels, but only use channels 1 through 11 in the U.S. In addition, the 802.11b standard recommends collocated access points be set to different channels with at least 30 MHz spacing. As a result, set the access points to channels 1, 6, and 11 if implementing three access points. For two access points, set to channels 1 and 6, 6 and 11, or 1 and 11.

Set each access point to a different service set identifier (SSID). The SSID differentiates one wireless LAN from another. As you take your access point out of the box (COTS), broadcast SSID is enabled, which means it will accept any SSID, therefore ensure default SSID is changed.

4. Frequency Management:

a. US and Possessions (US&P):

(1) Obtain installation spectrum manager authorization for use prior to WLAN purchase.

(2) If WLANs cause operational interference, they must cease operations and comply with AFI 33-118, *Radio Frequency Spectrum Management* and AFMAN 33-120 *Radio Frequency (RF) Spectrum Management* identifying WLANs as FCC Part 15 non-licensed devices.

b. Non-Licensed devices are illegal to operate outside US&P without prior frequency approval and assignment by Host Nation, and attendant frequency restrictions when used in other nations. DD Form 1494, Application for Equipment Frequency Allocation, must identify all anticipated operating locations, including US&P locations.

5. Standardization:

There are multiple standards currently in use and under development.

a. Follow Institute of Electrical & Electronics Engineers (IEEE) 802.11, 802.11a (5GHz), IEEE 802.11b (direct-sequence spread spectrum WLANs) currently approved standards.

b. Follow IEEE 802.11 (e) and (g)-- (128 MBPS encryption), IEEE 802.1X - an Extensible Authentication Protocol (EAP) - (for controlled port access) -- used as an extension to Remote Access Dial-IN User Service. (RADIUS) when these standards are approved.

c. Establish WLAN Continuity of Operations Plans (COOP) procedures in case of system failure.

d. Use replaceable Personal Computer Memory Card International Association (PCMCIA) cards, International Standards Agency (ISA) cards, Peripheral Component Interconnect (PCI) cards, or Universal Serial Bus (USB) connection devices.

6. Procurement:

Must comply with AFI 33-103, *Requirements Development and Processing*, and be approved by:

a. Functional systems: Approved by the Configuration Control Board.

b. Base-level systems: Approved by the local Host Wing Commander (WG/CC).

7. Sustainment:

Required through local contract(s)

Section 2 - Personal Digital Assistants (PDAs):

8. Application:

PDAs are information systems and subject to the same AF policy and guidance governing security and use of other information systems (i.e., desktop, notebook computer, etc.)

Users are authorized to use Blackberry type applications as long as email services remains in government hands, and you are not using a “store” and “forward” service.

Most wireless PDAs use some form of a commercial ISP. Commercial ISP service is allowed as long as transmission (encryption) security requirements are strictly adhered to.

a. Individuals may use PDAs to:

(1) Process unclassified information from desktop workstations. This includes the following typical features: schedules, contact information, notes, E-mail, etc.

(2) Take notes, save information, or write E-mails, when away from desktop workstations, whether down the hall or out of the country.

(3) Synchronize information with desktop workstations.

b. Do not use PDAs for the following:

(1) To process or maintain classified information.

(2) To dual auto synchronize personal PDAs on both your home computer and government computers, unless Air Force or DoD authorized licensed PDA anti-virus software is installed on the PDA.

[Refer to www.cert.mil for approved wireless anti-virus software governed by DISA].

(3) To synchronize information across a network using a wireless connection. The configuration required to permit this functionality introduces unacceptable risks into a network--opening firewall ports and sending passwords in the clear. Exceptions to this restriction will be addressed on a case-by-case basis and require local DAA approval.

9. Operations:

a. Disable auto sync on desktop application menu until needed. Install Air Force or DoD

authorized/licensed PDA anti-virus checking software. Once PDA and computer have

synced, turn off auto sync.

b. Disable IR port beaming capability. If IR port can not be disabled, cover with a visor or similar objects like black electrical tape.

c. Disable RF transmission capability (if it exists). A special consideration for security is important in a wireless network since radio frequency permeates the immediate transmission area. A direct physical link is not necessary to receive radio frequencies and therefore protection against eavesdropping is imperative. This is especially critical for devices running Bluetooth, which operates at nearly the same frequency as 802.11 devices, and will interfere with DSSS within ten meters of physical distance.

d. Turn off PDAs when not in use.

e. PDA guidance restricts PDA cradle connectivity and hot sync to government official mailboxes on computers within secure network environments where classified work is conducted.

f. Do not synchronize the PDA remotely by direct dial-in access to desktops. Ensure PDA connection through a remote access server (RAS) account is protected by an authorized network control center firewall.

g. To prevent the proliferation of Trojan Horse programs and other computer viruses that PDAs may be susceptible to, install Air Force or DoD authorized/licensed PDA anti-virus checking software.

10. Security:

Theft or inadvertent loss increases the risk of compromising classified or sensitive information.

a. Password protect PDAs according to AFMAN 33-223, *Identification and Authentication.* If PDA is unable to use a password, then increase physical access controls to prevent unauthorized access. To ensure protection of sensitive data on PDAs, strong security must be implemented. Password protection alone is insufficient. The critical element for the successful deployment of mobile devices throughout the corporate enterprise is an effective mobile data-management solution.

b. Include PDAs in the Network System Security Authorization Agreement (SSAA). Ensure vulnerabilities are included in threat and vulnerability assessment. Reflect handling, controlling and usage of PDAs in network security policy.

c. If individuals have a requirement to use a PDA on the AF network, they must first request a government-owned PDA. If a government owned PDA is unavailable, (and mission requirements dictate the use of a PDA), the DAA must approve personal PDA use.

Personal PDAs will not be connected to the Air Force network without justification and DAA approval. Justification must include mission requirements, government availability, and rationale of how duty position will be enhanced. Privately owned PDAs should be of the same operating system as the government procures/supports. Include handling of privately owned PDAs and software in the SSAA. Also, individuals must sign a PDA usage statement (Atch 2) agreeing to the terms in AFI 33-202, Computer Security, and include Telecommunications Monitoring and Assessment Program (TMAP) monitoring notice as part of the issuing documentation.

d. Do not use PDAs in classified [Emission Security] environments, because of their infrared and similar recording capabilities. PDAs should not remain connected via IR for extended periods of time, as an external source may gain access remotely. Techniques exist which permit an adversary the capability to capture information displayed on the PDA screen from greater than expected distances. Many users assume that the 802.11b signals only travel a relatively short distance, about a hundred feet or so. They actually travel much further, but are too weak to be detected by the tiny antenna in laptop cards.

e. Empty PDA cradles, when attached to a user PC, can be used to clone a PDA. Care should be taken to physically secure a cradle, when not in use.

f. PDAs (includes privately owned) contaminated with classified information will be confiscated by the organization commander or designated representative, and possibly destroyed, since there is currently no means to sanitize PDAs.

11. Procurement:

(Base level) requires WG/CC approval

WLANs: GSA, local contract

PDAs: AFWAY, IMPAC cards

12. Sustainment:

a. Government issued PDAs will be tracked in the Information Processing Management System (IPMS), per AFI 33-112, *Computer Systems Management*. Personal PDAs will be tracked by the Information Security Systems Officer (ISSO) and under the auspices of the local DAA. It is highly recommended each organizational commander establish proceduresto identify and turn in government issued PDAs prior to user's discharge or Permanent Change of Station/Permanent Change of Assignment.

b. Asset tracking and custodial responsibilities for these items are the responsibility of the organization commander or designated representative.

Section 3 - General

13. Research and Development

Report any issues, concerns, product evaluations, and lessons learned to HQ AFCA/GCLD for inclusion in AFCA research, development efforts and future policy releases.

14. References:

- AFI 33-103, Requirements Development and Processing
- AFI 33-112, Computer Systems Management
- AFI 33-118, Radio Frequency Spectrum Management
- AFI 33-201, Communications Security (COMSEC)
- AFI 33-202, Computer Security
- AFI 33-203, Emission Security
- AFMAN 33-120, Radio Frequency (RF) Spectrum Management
- AFMAN 33-223, Identification and Authentication
- FIPS Pubs 140-1, Security Requirements for Cryptographic Modules
- FIPS Pubs140-2, Advanced Encryption Standard (AES)

Attachment 2 (Added)

IA VIOLATION DECISION MATRIX

(Offenses within a 12-month period)

Any User	**1st Offense**	**2nd Offense**	**3rd Offense**	**>3 Offenses**
Incorrect use of authorized modem on PC connected to base network (concurrent network and modem connection)	Memo to organization reminding them of the proper procedures for use.	Disable individual's account and block that IP from the network. Memo to organization CC of offense. Offender briefs organization CC.	Memo to organization requiring individual and organizational commander explain in person to wing/center CC that the individual will not have any more violations within the 12-month period from the 1st offense and explain why the individual should be allowed access to the network.	Same as 3rd offense, with consideration to not allowing individual access to the base network for an extended or indefinite period.
Adding unauthorized external connection to PC or subnet connected to the base network.	Disconnect at the appropriate level (circuit/ subnet/PC). Send memo to organization of violation.	Disconnect at the appropriate level (circuit/subnet/ PC). Send memo to organization of violation. Offender briefs organization CC.	Disconnect at the appropriate level (circuit/subnet/PC). Send memo to offending organization requiring the offender and the organization commander explain the situation to wing/ center commander.	Same as 3rd offense, with consideration to not allowing individual and org. CC access to the base network for an extended or indefinite period.
Sending classified over the unclassified network.	Disable users account. Send memo to organization of violator.	Disable users account. Send memo to offending organization requiring the offender and the organization CC to brief the wing/center CC.	Same as 2nd offense, with consideration to not allowing individual access to the base network for at least 30 days or an indefinite period of time.	Same as 3rd offense, do not allow individual access to the base network for an indefinite period.

Any User	1st Offense	2nd Offense	3rd Offense	>3 Offenses
Using streaming audio or video or other improper use of network bandwidth for other than mission related requirements, i.e. listening to radio station over the network, sports casts, etc.	Disable users account. Send memo to organization of violation.	Disable users account. Send memo to the offending organization requiring the organization CC to brief the wing/ center CC.	Disable users account. Send memo to the offending organization requiring the offender and the organization CC and the offender brief the wing/center CC.	Same as 3rd offense, with consideration to not allowing individual/organization CC access to the base network for an extended or indefinite period of time.
Extended (over 1 minute at one site) visits/repeat visits to the same site/downloading pornographic material from the Internet.	Disable users account. Send memo to organization of violation requiring the offender and the organization CC brief the wing/center CC. Consider OSI involvement	Disable users account. Send memo to offending organization requiring the offender and the organization CC brief the wing/center CC. Contact OSI to investigate the incident.	Permanently disable the users account. Send memo to organization of violation informing the offender and the organization commander to begin removal personnel action.	N/A

System Administrators	1st Offense	2nd Offense	3rd Offense
System Administrator policy noncompliance resulting in CAT I/II intrusion.	Offending System Administrator loses privileges until IA retraining is completed. Unit CC verify that unit System Administrator(s) complete required actions.	System Administrator loses privileges for up to 4 weeks. Offending unit CC briefs wing/center CC.	Permanent Removal of System Administrator privileges for offending System Administrator.

Attachment 3 (Added)

EXAMPLE MEMORANDUM OF POLICY VIOLATION NOTIFICATION

EXAMPLE MEMORANDUM
OF
POLICY VIOLATION NOTIFICATION

MEMORANDUM FOR 557 ABW/DO

FROM 557 ABW/CC

SUBJECT: 1ST Policy Violation by *Name of offending individual, office symbol*

1. *Name of offender, office symbol* has violated network policy by *specify offense* (example downloading files from an unauthorized pornographic site, or installing an unauthorized modem on networked computer, sending classified material over the unclassified network).

2. Please ensure the individual receives computer and network remedial training to preclude future violations.

3. (Optional paragraph dependent on whether or not individual's account was disabled) *Name of offender's* network account has been disabled until we receive a memorandum signed by the organizational commander requesting the account be enabled and stating the individual has successfully completed computer and network remedial training.

cc: Security Forces Unit Commander
Communications Unit Commander

Attachment 4 (Added)

GUIDE/FORMAT

FOREIGN NATIONALS ACCESS REQUESTS

(FOR SUBMITTAL IN COMPLIANCE WITH AFI 33-202, PARA 3.7.1)

1. The following information is required of the sponsoring organization and will be submitted via the Base Information Assurance Office to HQ AFMC/SC for review and staffing to AFMC/CV. Required information must be provided as attachments to AF Form 1768 (staff summary sheet). Requested information is consistent with requirements identified by SAF memo, "Foreign National Access to Information Systems", dated 31 Jul 1998.

a. Requesting organization must ensure that information to be accessed by foreign nationals is properly processed for disclosure and that systems accreditation authorities concur with the access. Therefore, as attachment one to the SSS, the requesting organization must provide a memorandum that includes justification detailing the requirement for access, type of information to be accessed, expected duration of access, and category of the position the subject will occupy IAW DoD 5200.2-r, appendix k. Additionally, the memorandum must be coordinated locally via staff summary sheet (SSS) showing coordination by the servicing foreign disclosure office (FDO), the servicing information security program manager (ISPM), the Designated Approval Authority (DAA) for the network to be used, the unit security manager (UCM), and the local information assurance (IA) office. The local IA office should be the last agency to coordinate on the package. Paragraph 2 below provides additional guidance regarding FDO, ISPM and UCM coordination.

b. Ensure the certification and accreditation documentation for the system is updated to reflect foreign national access. Therefore, as attachment 2, provide a copy of the System Security Authorization Agreement. The DAA must ensure that the SSAA includes the following:

(1) The Unit COMPUSEC Manager (UCM) and the Information System Security Officer (ISSO) have the computer security procedures in place to assure that only authorized information is accessible, as defined by the foreign disclosure office.

(2) Inclusion of the risk and vulnerability assessment, which must address the potential vulnerability of access by foreign nationals. It must define the system/network safeguards present to ensure that the foreign national has permission to access only the types/categories of information determined to be releasable by the servicing foreign disclosure office.

(3) Coordination by the local IA office.

c. Package must ensure security measures employed adhere to information protection policy. Therefore as noted above (paragraph 1) the HQ AFMC IA office will review the package to ensure completeness and obtain coordination from HQ staff as appropriate, and forward the request with AFMC/SC recommendation to AFMC/CV.

2. Coordination on the SSS by the FDO, ISPM and UCM will ensure the following:

a. The servicing Information Security Program Manager (ISPM) will verify via coordination on the SSS that an individual has received a favorable personnel security investigation (PSI), either single scope background investigation (SCBI) or National Agency Check (NAC). If the ISPM is unable to verify a

current, favorably completed PSI, they will notify the sponsoring organization. The sponsoring organization will decide whether or not to submit a request for a PSI to the ISPM. (Note: There are no provisions for interim access by foreign nationals. The PSI action must be completed and access determination made by the sponsoring organizational commander prior to submitting this package.)

b. The unit security manager will coordinate on the SSS to verify that the information requirements identified in AFI 33-202, section 3.7. have been addressed.

c. The servicing foreign disclosure office coordination will verify that the types/categories of information requested are releasable

DEBORAH L. HALEY, SES
Director of Communications and Information